

Dear Rhode Islanders,

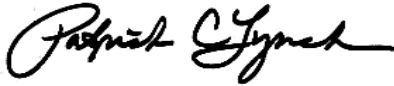
Whether you are a high school student, a senior citizen, or someone in between, you are an integral part of the American economy. You are the consumer. From the goods and services you purchase, to the charities you sponsor, you collectively spend tens of billions of dollars annually. As such, you possess great power. With great power, though, comes great responsibility. You must do all that you can to educate and protect yourself. As your Attorney General, I would like to help you navigate through the often difficult choices you are faced with on a daily basis and provide resources in the event you find yourself the victim of fraudulent or deceptive practices.

It is in this spirit that I am happy to publish “Navigating Your Way Through The Consumer World— *A How-to Guide For Today’s Consumer*”. This guide is a compilation of facts and guidelines gathered from the Federal Trade Commission and covers the following issues: Basic Consumer Protection, Scams, Charities, Telemarketing, Identity Theft, and Business On The Web.

As always, my Consumer Protection Unit is here to assist you when you need to file a complaint. It is my hope, however, that this

resource guide will help to prevent some of those complaints by arming you with the best form of prevention... information.

Sincerely,

A handwritten signature in black ink, reading "Patrick C. Lynch". The signature is written in a cursive, flowing style with a prominent initial "P" and a long, sweeping underline.

Patrick C. Lynch
Attorney General

TABLE OF CONTENTS

SECTION I: TELEMARKETING	
<i>What To Do About Unsolicited Calls</i>	5
 SECTION II: CHARITIES	
<i>How to Give Without Being Taken</i>	11
 SECTION III: SCAMS	
<i>When To Say No To A Great Sounding Offer</i>	14
 SECTION IV: BUSINESS ON THE WEB	
<i>Advice For Information Age Shoppers</i>	19
 SECTION V: IDENTITY THEFT	
<i>Keeping Your Personal Information Personal</i>	21
 SECTION VI: CONSUMER PROTECTION	
<i>It Begins With You</i>	26

TELEMARKETING

What To Do About Unsolicited Calls

Telemarketing fraud is a multi-million dollar business in the United States that can affect the youngest consumer to the oldest. Scam artists do not discriminate between individuals; they will try to scam who ever they can. Believe it or not there is no typical fraud victim. Research has shown that fraud victims are likely to be educated, informed, relatively affluent, and involved in their communities. Telemarketing scams can originate by telephone, mail, or even in the marketplace and it is very important to be a proactive consumer to try and protect yourself. The key to protecting yourself from telemarketing fraud is learning how to detect a scam artist, and know the differences between a legitimate and fraudulent offer.

With the enactment of the federal regulation known as the “Telemarketing Sales Rule”, in 2003, this acts as further protection for consumers in dealing with various telemarketing problems. The regulations provide additional help for consumers receiving various phone calls, as well as unwanted sales solicitations. Most types of telemarketing calls made to residential

consumers fall under the restrictions created by the regulation. Keep in mind, however, that certain calls, such as calls from charities, telephone surveys and from businesses with which you have an existing relationship are NOT restricted by the regulation.

The Do Not Call Registry

- One of the best ways to reduce the amount of telemarketing calls is to sign up for the Federal Do Not Call List. Please remember that telemarketing scam artists are not law abiding, and may still call you, even if you number is registered.
- Sign up for the Do Not Call List by dialing **888-382-1222**. When registering by phone, you must call from the number you wish to have registered. You may also register online at www.donotcall.gov. You must have a valid email address to use this service. After registering, you will receive an email with a link that must be clicked on within 72 hours to finalize the registration process. This registration will last for five (5) years.

Other Ways to Protect Yourself From Telemarketing Calls

- You also have the option of Company-Specific Do-Not-Call Lists. You may make a direct request to a specific person or entity calling to cease their calls. You must make a separate do-not-call request to each telemarketer from whom you do not wish to receive calls. When you receive unwanted solicitation calls, specifically state that you want to be added to the caller's do not call list. The FCC advises you keep a list of persons and businesses you have asked not to call you.

Main Regulations of the Telemarketing Sales Rule

- Telemarketers may only call you between the hours of 8am and 9pm.
- Telemarketers must tell you it is a sales call, as well as who is doing the selling, *before* they make their pitch.
- If the call concerns a prize promotion, a telemarketer must tell you the odds of winning, any restrictions or conditions of receiving the prize, and that no purchase is necessary to enter or win.

Remember- *if you are asked to pay for a prize just hang up!*

- Telemarketers must tell you the total cost of the products or services offered, any restrictions on receiving or using them, and whether a sale is final or nonrefundable, *before* you pay.
- Telemarketers must have your express and verifiable authorization in order to withdraw money from your checking account.

Red Flags of Telemarketing Fraud

- If an offer sounds ***too good to be true***, it probably is!
- A ***demand*** that you must act quickly, or the use of scare tactics to buy or agree to a good or service.
- A ***refusal*** to send you a written documentation before you accept the offer.
- ***Insistence*** that you wire money, provide your bank account information, or have a courier pick up your payment.
- A ***refusal*** to stop telephone contact with you.

If you recognize any of the red flags, hang up!

Tips to Remember

- Do not fill out contest entry forms at fairs or malls—they are a common source of leads for telemarketers and con artists. Ask companies you do business with not to share your personal information with other marketers.
- Know your rights under federal law. You can tell a telemarketer not to call you again.
- Know with whom you are dealing. Check with the Department of Business Regulation, or contact the Better Business Bureau if a company or charity is unfamiliar to you.
- Screen your phone calls by using an answering machine, or caller ID. Other services may be available through your phone company.
- Have a plan for speaking to telemarketers. Before you pick up the phone, know what questions to ask, or what you want to say. Determine what information you are willing to divulge to a telemarketer. During a call, be polite, but firm. Hang up if someone refuses to answer your questions or you detect any of the “red flags.”

To File Complaints or for More Information

- The FCC provides several ways for consumers to file complaints. You may file a complaint using an electronic complaint form at <http://www.fcc.gov/cgb/complaints.html>. You may also send an email to donotcall@fcc.gov. To file a complaint over the phone you may call 1-888-CALL-FCC (1-888-225-5322) voice or 1-888-TELL-FCC (1-888-835-5322) TTY.
- For more information, log onto the FCC's website at www.fcc.gov.

CHARITIES

*How to **Give** Without Getting **Taken***

Most charities are worthy of your financial support. Charitable fundraising, however, is a big business these days, and just like any big business, it has its share of questionable operators. In today's economy it is more important than ever to make your donations carefully. Therefore, before making your next donation, follow the tips provided below.

THINGS TO REMEMBER

- Ask for written information about the charity, including name, address and telephone number. A legitimate organization will give you information about the charity's mission, how your donation will be used, and proof it is tax deductible.
- Research the organization on the BBB Wise Giving Alliance website (www.give.org), or call the Department of Business Regulation (401-222-2246) to ensure its legitimacy. Beware of "sound alike" organizations who may also solicit for a donation, relying on the good name and reputation of another organization.

- Ask how much of the contribution goes to fundraising or administrative expenses, and how much is left for the cause you want to support. Recognize that professional fundraisers are entitled to a portion of the money they raise. If you are uncomfortable with the percentage the fundraiser retains, mail your check directly to the charity so they benefit from the full amount of the contribution.
- Keep records of your donations. Copies of checks, receipts etc., come in handy when filing tax returns or when filing a complaint.
- Never send cash. Pay by check and make it out to the charity, never the fundraiser. Use the charity's full name rather than its initials.
- Never give your credit card number to a fundraiser over the phone unless you are absolutely certain with whom you are dealing.
- Be wary of organizations that offer to send a courier or overnight delivery service to collect your donation. This is a common vehicle for scam artists who wish to make off with your money. If this service is offered make sure you are home during the pick up time, and ask for proper identification.

- Do not succumb to a high-pressure appeal or “sob story”. The need will always be there, so research first and give later.

SCAMS

*When To Say **NO** To A Great-Sounding Offer*

Con artists have turned fraud into a multi-billion dollar business. Each year, thousands of consumers lose anywhere from a few dollars to their life savings to scams. Once the money is gone, it is often very difficult, if not impossible, to recover.

Though anyone may fall victim to a con artist, criminals often target individuals ages 60 or older. Con artists operate under the theory that older individuals are more trusting and polite, have expendable incomes, and are home during the telemarketing hours between 8 am and 9 pm, Monday thru Sunday.

Common Scams

- ***Nigerian Letter Scam or 419 Scam-***
Circulated primarily via email and fax, these scams can take shape in a variety of ways. Frequently, a letter is addressed from a foreign individual, often posing as a government official, prince, or some other individual, seeking to transfer funds to the United States overseas. The sender requests that you help

pay for the transaction costs and promises to compensate you with a percentage of the total sum. Many times, a check will accompany the letter, asking the recipient to cash it and wire transfer some of the money back to the sender. The origin of these letters cannot be traced and therefore, consumers who lose money will not be able to recover it.

- ***Free Gifts, Free Vacations, and Prize Offers-*** You usually have to give something in exchange for the “free offer.” Often times you will pay more than the promotion is actually worth. Make sure to get all of the details upfront and in writing. Do not pay any upfront fees!
- ***Investment Opportunities-*** From timeshares to rare jewels, oil, and other treasures, these opportunities are offered as “once in a lifetime” ways to make thousands of dollars at no risk to you. As a rule, these “get rich quick” schemes are worthless.
- ***International Lottery Schemes-*** Most foreign lottery offers are phony, designed to deceive the consumer into giving monies or personal and credit information, which could later result in credit fraud or identity theft. Playing a

foreign lottery is also against federal law.

- ***Work at home-*** These schemes guarantee a stable income working in the comfort of your own home. Beware, for usually the consumer has to cover the “start up costs” (ie. computer software, materials), which can cost hundreds or even thousands of dollars.
- ***Advance-Fee Loan Scams-*** Fraudulent loan brokers and mortgage companies guarantee consumers credit and mortgages in exchange for an upfront fee. Check with the local licensing board before doing business with loan brokers or mortgage companies. Requiring upfront fees is illegal.
- ***Recovery Scams-*** “Recovery room” operators contact consumers who have been the victim of a scam and promise to recover their lost money and prizes for a fee. These operators require the consumer to pay for their services in advance. Once the consumer pays, the recovery operator never contacts the consumer again.
- ***Internet Auction Scams-*** When selling items online, do not ship the merchandise until you have confirmed that the buyer’s check has

cleared. If a check is sent for more than was owed, and the buyer is requesting you send the monetary difference with the merchandise, **BEWARE!** A popular scam is on the rise involving fraudulent bank checks. Though the checks appear authentic and may be accepted by the bank initially as legitimate, they are actually counterfeit. Those who fall victim to the scheme lose not only their merchandise, but also the monies they forwarded to the supposed “buyer.” The perpetrators are usually situated outside of the U.S. and therefore, the likelihood of reclaiming your hard earned dollars is extremely slim.

THINGS TO REMEMBER

- If you have won something you should not have to pay a single penny. Being asked to pay for shipping/handling, taxes, delivery, etc. is a sure sign the offer is a scam.
- Ask yourself, why would a perfect stranger pick me? Why would I share my personal banking information with anyone?
- Do not buy from an unfamiliar company. Ask for the company’s contact information. Legitimate companies understand your desire to

know more and willingly comply; scam artists will stall or refuse.

- A legitimate company will not pressure you into making snap decisions. It will provide you with extensive information about the product/prize offer, and ample opportunity to ask questions. Resist pressure to “act immediately.”
- If possible pay with a credit card. If something goes wrong you can dispute it with the credit card company.

WHERE TO FILE COMPLAINTS

- Contact either the Consumer Protection Unit, or the Federal Trade Commission (877-382-4357 or www.ftc.gov) to report the incident and file a complaint.
- If you have paid with credit or debit cards, contact the card issuer to dispute the charges.

BUSINESS ON THE WEB

Advice For “Information-Age” Shoppers

With the advent of personal computers, today’s consumer is faced with a whole world of buying opportunities. With the simple click of a mouse, the purchasing possibilities are endless.

Shopping electronically, especially when you are dealing with an unfamiliar vendor, also opens up a whole world of questions and potential challenges. Is the company legitimate? Was the product or service accurately advertised? Will unexpected charges be added to the price? If there’s a problem, where can you get it resolved?

THINGS TO REMEMBER

Browser Security- Make sure you have a browser that encrypts all information you send over the web. This impedes hackers from being able to access your credit card and bank information.

Research Company Legitimacy- Get the company’s physical address, telephone number, and country where it is based.

Payment Options- Never send cash. Use a payment method allows you to keep record of the transaction.

Know the Company's Policies-

- **Privacy & Security Information-**
Read the privacy and security policies. Does the company ensure the privacy of your personal information? Does it send your information over a secure connection? Does the company sell/share customer information with other companies? If so, you have the choice to opt out?
- **Refunds & Returns-** How long do you have to return an item? Does the company give refunds? If so, what percentage will you be refunded? If not, do they give credit you can use toward the purchase of a different item?
- **Shipping & Handling/ Delivery Costs-** Upon purchase, who pays for the delivery of your item?

For Help with E-Commerce Crimes:

- Contact the FTC (877-382-4357) or contact the Internet Fraud Complaint Center at www.ic3.gov.

IDENTITY THEFT

Keeping Your Personal Information Personal

Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information without your permission to commit fraud or other crimes.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years, and their hard earned money, cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they did not commit.

Minimize Your Risk

- Order copies of your credit report each year to check if your information is correct. Your credit report contains information on where you work and live, the credit accounts you have opened in your name, how you pay your bills and whether you've been sued, arrested or filed for bankruptcy. You may

access a free copy of your credit report by calling the toll free number, 877-322-8228 or via the website www.annualcreditreport.com.

- Rhode Island residents can place a security freeze on their accounts with the credit bureaus. A security freeze prohibits credit-reporting agencies from releasing personal credit report information. A consumer must send a certified letter by mail to each credit bureau requesting the freeze. There is a nominal fee to each of the agencies to place the freeze on your account. However, the fee is waived for victims of identity theft and for those over the age of 65. With a security freeze in place, a company is prohibited by law from releasing any information in the credit report without the express authorization or approval of the consumer.

Tips to Help Prevent Becoming a Victim

- Place passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name,

your birth date, the last four digits of your SSN or your phone number.

- Do not disclose your personal information—such as your address, telephone number, SSN, bank account number or email address—unless you know who’s collecting the information, why they are collecting it and how they will use it.
- Do not carry your social security card with you and always secure your personal information in your home, especially if you are having any service work done.
- Shred all documents before you throw them away, especially those that contain personal information.
- Pay attention to your billing statements and immediately report any fraudulent charges. Also, pay attention to the delivery date of your bank and credit card statements when you receive them each month.
- Protect information stored on your computer by using passwords, regularly updating your virus software, using secure browser the

encrypts all information you send over the Internet, and reading the privacy policy of websites you visit. Do not download files sent to you by strangers or click on unknown hyperlinks.

IF YOU ARE A VICTIM

- Contact the fraud departments of any of the three major credit bureaus, Experian (888-397-3742), Equifax (800-525-6285) and TransUnion (800-680-7289), to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three-credit reports will be sent to you free of charge. The fraud alert will last 90 days, and can be extended after the 90 days for seven years when notified in writing.
- Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Affidavit when disputing new authorized accounts.

- File a police report. Get a copy of the report to submit to your creditors and other that may require proof of the crime.
- File your complaint with the FTC (877-382-4357). The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations.
- Keep records of all phone calls, reports filed, correspondence, ect. and follow up phone conversations with certified letters.
- Contact the Department of Attorney General, Consumer Protection Unit (401-274-4400).

CONSUMER PROTECTION

It Begins With You!

Consumer protection is largely self-protection. Before you make any retail purchase or enter into a contract, you must learn and understand your individual rights and responsibilities.

Knowing these things can help prevent you from becoming a victim of fraud, deceit, or simple misunderstanding. It is far better *to not allow* yourself to be taken advantage of in the first place, than it is to have to ask for help in getting restitution after the fact.

Take a moment and reflect on the events of your busy day. Perhaps you entered your PIN number for your debit card at the grocery store, mailed a check for your utility bill, purchased a gift online, or ordered theater tickets over the phone. With each transaction, you are revealing bits of your personal information, such as your name, address, telephone number, Social Security Number and banking information. To you this is part of a daily routine, but to an identity thief this is hitting the jackpot.

Becoming a smart and savvy consumer does not mean changing your daily routine; it involves becoming more aware of how to

prevent becoming a victim. As the saying goes, “knowledge is power.” The best way to protect yourself is simply being aware of scams and the ways identity thieves operate, and practice responsible consumer habits.

THINGS TO REMEMBER

Read Carefully before you buy or sign

- Read the fine print in any advertisement before you buy a product.
- Always remember to read any “Agreement” or “Contract” carefully before you sign it. These documents are almost always legally binding. Failure to honor your legal obligations can have serious and long lasting consequences for you!
- Get a written copy of guarantees and warranties and make sure you understand their terms and conditions.

Refund Policies

- Rhode Island law states that consumers are entitled to a refund in the same manner as paid if returned within ten (10) days with a sales slip. Retail stores are also entitled to their own store policy, however they are required to post their refund policies in a conspicuous place: at store

entrances, at the cash register, or at the point of display. The law does not say what the policies must be unless the product is defective. This decision is left to the store.

- Before making a purchase, ask about the store's specific refund, return or exchange policies.
- Beware of "buyers' remorse." Do not be misled into thinking that you have an automatic "cooling off" or cancellation period when making a purchase. (Be aware that this includes the purchase of an automobile.)

Gift Certificates-

- With the exception of prepaid wireless telephone cards, businesses are now no longer allowed to place expiration dates, service or maintenance fees on gift certificates.

Compare and research before you buy

- "Comparison shop" for goods and services whenever possible.
- Before committing a large amount of money for the purchase of a "big ticket" item, such as an automobile, research the business with the Better Business Bureau of Rhode Island (BBB) (www.bbb.org or 401-785-1212). The BBB staff should be able

to tell you the complaint history of the business and whether or not these complaints have been satisfactorily resolved.

Documentation helps when filing a complaint

- Save “proof of purchase” documentation such as sales slips, credit card receipts, or cancelled checks. Whenever you file a complaint with any business or agency, be sure to keep copies of any correspondence and supporting documentation you send to them.

WHERE TO FILE COMPLAINTS

- You can contact the Consumer Protection Unit of the Rhode Island Department of Attorney General (401-274-4400 or contactus@riag.ri.gov) to file a consumer complaint against a Rhode Island business. We answer consumer questions, mediate complaints or suggest where you might go to get help. We are not authorized to give legal advice or business references.
- The BBB will take a complaint from you about a business in Rhode Island. If you buy something from a business located in another state, and

you have a problem, the BBB of Rhode Island can give you the contact information for the nearest affiliate.

- Rhode Island has a Small Claims Court (401-458-5402), a part of the District Court system. If you have a claim against a Rhode Island business that fails to address your complaint to your satisfaction, you may be able to take it to Small Claims Court for a small filing fee. Small Claims Court allows you to handle your own case without the need for an attorney.
- Finally, you have the option of consulting with and hiring a private attorney to represent you.

